UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/742,329	12/19/2003	Bruce L. Brown JR.	022395-005800US	5765

46670 7590 08/31/2007

TOWNSEND AND TOWNSEND AND CREW LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER	
CHAN, CHRISTOPHER T	
ART UNIT	**PAPER NUMBER**
2146	

MAIL DATE	DELIVERY MODE
08/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/742,329	BROWN ET AL.	
	Examiner	Art Unit	
	Christopher Chan	2146	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *4-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 December 2003* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/19/2003*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☒ Other: *NPL Documents*.

DETAILED ACTION

1. The instant application having Application No. 10/742,329 has a total of 19 claims pending in the application; there are 3 independent claims and 16 dependent claims, all of which are ready for examination by the examiner.

Oath/Declaration

2. The applicant's oath/declaration has been reviewed by the examiner and is found to conform to the requirements prescribed in **37 C.F.R. 1.63.**

Information Disclosure Statement

3. As required by **M.P.E.P. 609(C)**, the applicant's submissions of the Information Disclosure Statement dated December 19, 2003 is acknowledged by the examiner and the cited references have been considered in the examination of the claims now pending. As required by **M.P.E.P 609 C(2)**, a copy of the PTOL-1449 initialed and dated by the examiner is attached to the instant office action.

Drawing Objections

4. Figures 1-3 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). Corrected drawings in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. The replacement sheet(s) should be labeled

"Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-2, 8, and 15 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding Claims 1 and 8, Applicant claims identifying a "possible spoofed connection." The use of the term "possible" under this phrase renders this claim indefinite to one of ordinary skill in the art as it can not be determined as to whether a connection is actually a spoofed connection or not.

Regarding Claims 1-2, 8, and 15, Applicant claims delaying messages for a "delay period," however such a delay period is not specified exactly nor is a set range provided in any of the claims or in the specification ("such as 3-5 seconds" in [0033] implies that it can be a time outside 3-5 seconds as well). Only examples of times are used but none can be seen as a time that would distinctly establish a delay time that will

work for the invention as disclosed. A spoofing MTA/MUA may also have a designated time for message response waiting that varies which would make a delay simply a "delay period" indefinite as well. For the purposes of examination, the Examiner respectfully interprets this as being any kind of delay period.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,654,787 (hereinafter Aronson et al.) further in view of "The Next Step in the Spam Control War: Greylisting" (hereinafter Harris).

Regarding Claim 1, Aronson et al. taught a method for a mail server using Simple Mail Transfer Protocol (SMTP) on a network with User Agents (or MUAs) such that spam or unwanted mail can be filtered and stored in its own spam storage area **(Col. 3, Lines 21-40, Col. 5, Lines 2-20)**.

In respect to Claim 1, Aronson et al. taught the method set forth above except for the method implemented amongst such a framework so that a spoofed network connection (or spam sender) can be detected by receiving a client connection, delaying

the transmission of a greeting message for a certain period, monitoring the connection during that period, and if a command is received from the client prior to a greeting message, identifying the connection as a possible spoofed connection. Since Aronson et al. already teaches that its method identify spam as they arrive from any client connection and filter them before they are sent to a recipient, one of ordinary skill in the art would easily agree that such a method wastes mail server resources by processing such spam filtering from any e-mail sender. By actually preventing the sender from sending such a message in the first place to the mail server, it would obviously reduce the processing load on the mail server and client application on the receiving user agent. It would also reduce the amount of maintenance required in storing such unwanted electronic messages. Harris teaches of a method in the similar endeavor of anti-spam amongst e-mail networks wherein the method runs on the Message Transfer Agent level (mail servers/users using SMTP like Aronson et al.) that is designed to complement other spam control systems and not as a direct replacement **(Harris Page 1, Last Paragraph. Page 2, 3rd Paragraph)**. In the Greylisting method taught by Harris, a mail server that uses it **(Harris Page 2, 2nd Paragraph)** will look at data called triplets which include an IP address and sender/recipient address. Any time such a triplet is not seen before by the server, delivery is refused initially **(Harris Page 2, 2nd Paragraph from bottom to Page 3, 2nd Paragraph; all new connections are essentially assumed to be spammers, or spoofed connections, and are "delayed" for some delay period by not having their connection received. Harris Page 4, command sequences; commands from the unknown address are received for**

mail delivery in SMTP form, but commands are received prior to a 250 greeting message and are given a tempfail as per the implementation suggests) until the server sees that retries are attempted (so it can prove it's not a fire-and-forget spammer) wherein it will then pass the e-mail **(Harris Page 5, outline of implementation; during this delay, the mail server is monitoring the connection, particularly for retry attempts wherein the mail pass due to retries signal the end of the delay period)**.

It would have been obvious for one of ordinary skill in the art at the time the invention was made to combined Aronson et al.'s disclosed invention with the Greylisting method as taught by Harris as Greylisting is a well-known method already implemented on mail systems at the time of invention that was designed specifically to complement other anti-spam methods as taught above. Such a method would also reduce the processing overhead of the mail systems by removing the need to process e-mails unwanted by a user without the use of any additional network resources as well. This combined invention of Aronson et al. and Harris was always an option that a mail administrator can choose to implement on his or her network of interest.

Regarding Claim 2, Aronson et al. together with Harris taught the method further comprising: sending the greeting to the client upon completion of the delay period **(Harris Page 5, Outline; mail and thus connection greetings, etc. are conducted and passed normally following the delay period and retry attempts)**.

Regarding Claim 3, Aronson et al. together with Harris taught the method further comprising: processing any electronic mail associated with a spoofed connection **(Aronson et al. Abstract; mail server filters e-mail messages, therefore processes any e-mail, regardless of what type of connection it is)**.

Regarding Claim 4, Aronson et al. together with Harris taught the method wherein electronic mail associated with a spoofed connection is processed using a process selected from the group consisting of **(Aronson et al. Col. 4, Lines 57-67; spoofed connections, or spammers)**:

deleting a spoofed-connection electronic mail message **(Aronson et al. Col. 4, Lines 13-16; deletes marked messages, which obviously can be of spammer source)**;

marking a spoofed-connection electronic mail message **(Aronson et al. Col. 5, Lines 2-8; marked messages stored as spam, which would be of spoofed-connection source)**; and

storing a spoofed-connection electronic mail message in a special electronic directory **(Aronson et al. Col. 5, Lines 2-8; stored in its own spam storage area 230. Aronson et al. Col. 9, Lines 1-6; proxy form has its spam storage area too)**.

Regarding Claim 5, Aronson et al. together with Harris taught the method wherein the connection is a Transmission Control Protocol (TCP) connection **(Aronson et al. Col. 3, Lines 35-40; connections are TCP)**.

Regarding Claim 6, Aronson et al. together with Harris taught the method wherein the client is a Mail Transfer Agent (MTA) or Mail User Agent (MUA) **(Aronson et al. Col. 3, Lines 35-40; since SMTP is used, clients are inherently MTAs or MUAs. Aronson et al. Col. 3, Lines 21-30; user agent clients)**.

Regarding Claim 7, Aronson et al. together with Harris taught the method wherein the received command is a Simple Mail Transfer Protocol (SMTP) command **(Aronson et al. Col. 3, Lines 39-40; SMTP. Harris commands as taught above are in SMTP as well)**.

Regarding Claim 8, Aronson et al. together with Harris taught a method for detecting spoofed network connections comprising **(Harris Page 13, Possible methods of spammer adaptation 1st and 2nd paragraphs; mail server can detect any connection and apply for any, even if spammer spoofs its IP addresses)**:
receiving a first command at a server from a client **(Harris Page 4, second set of commands, RCPT command from client)**;
delaying, for a delay period, a transmission of a reply associated with the first command **(Harris Page 4, second set of commands, tempfail 451)**;
monitoring a connection between the server and the client during the delay period; and
if a second command is received at the server before the reply is transmitted, then identifying the connection as a possible spoofed connection **(Harris Page 5, outline of**

implementation; during this delay, the mail server is monitoring the connection, particularly for retry attempts wherein the mail pass due to retries signal the end of the delay period. This retry is a second command after the tempfail delay).

Regarding Claim 9, Aronson et al. together with Harris taught the method further comprising: sending a greeting to the client when the connection is established with the server **(Harris Page 4, two sets of commands; 250 greeting messages are sent on connection establishments or attempts)**.

Regarding Claim 10, Aronson et al. together with Harris taught the method further comprising: transmitting the reply upon completion of the delay period **(Harris Page 5, Greylisting outline; pass the e-mail after block expiration, or delay end)**.

Regarding Claim 11, Aronson et al. together with Harris taught the method further comprising: processing any electronic mail associated with the spoofed connection **(Aronson et al. Abstract; mail server filters e-mail messages, therefore processes any e-mail, regardless of what type of connection it is)**.

Regarding Claim 12, Aronson et al. together with Harris taught the method wherein the connection is a Transmission Control Protocol (TCP) connection **(Aronson et al. Col. 3, Lines 35-40; connections are TCP)**.

Regarding Claim 13, Aronson et al. together with Harris taught the method wherein the client is a Mail Transfer Agent (MTA) or Mail User Agent (MUA) **(Aronson et al. Col. 3, Lines 35-40; since SMTP is used, clients are inherently MTAs or MUAs. Aronson et al. Col. 3, Lines 21-30; user agent clients)**.

Regarding Claim 14, Aronson et al. together with Harris taught the method wherein the received command is a Simple Mail Transfer Protocol (SMTP) command **(Aronson et al. Col. 3, Lines 39-40; SMTP. Harris commands as taught above are in SMTP as well)**.

Regarding Claim 15, Aronson et al. together with Harris taught an apparatus for detecting spoofed connections comprising:

means for detecting when a connection is established between the apparatus and a client device **(Harris Page 13, Possible methods of spammer adaptation 1st and 2nd paragraphs; mail server can detect any connection and apply for any, even if spammer spoofs its IP addresses. Additionally the rejections as per Claims 1 and 8)**;

means for transmitting a greeting message or a reply or both to the client device **(Harris Page 4, both sets of commands; 250 greeting replies. Additionally the rejections as per Claims 1 and 8)**;

means for delaying the transmitting means for that the greeting message or the reply or both are not transmitted during a delay period **(Harris Page 4, second set of commands, tempfail 451. Additionally the rejections as per Claims 1 and 8)**; and

means for monitoring the connection to detect commands that are sent by the client device at least during the delay period **(Harris Page 5, outline of implementation; during this delay, the mail server is monitoring the connection, particularly for retry attempts wherein the mail pass due to retries signal the end of the delay period. Additionally the rejections as per Claims 1 and 8)**.

Regarding Claim 16 Aronson et al. together with Harris taught the apparatus wherein the client device is a Mail Transfer Agent (MTA) or Mail User Agent (MUA) **(Aronson et al. Col. 3, Lines 35-40; since SMTP is used, clients are inherently MTAs or MUAs. Aronson et al. Col. 3, Lines 21-30; user agent clients)**.

Regarding Claim 17, Aronson et al. together with Harris taught the apparatus wherein the detecting means, the transmitting means, the delaying means, and the monitoring means comprise one or more processor-based devices running software algorithms to provide the detecting, transmitting, delaying and monitoring functions **(Claim 17 is rejected for the same reasons as taught above as such means are inherently taught being operated by the computers, which inherently have processors, attached to the taught network. Aronson et al. teaches processor-based devices explicitly in Col. 2, Lines 61-67)**.

Regarding Claim 18, Aronson et al. together with Harris taught the apparatus wherein the connection is a Transmission Control Protocol (TCP) connection **(Aronson et al. Col. 3, Lines 35-40; connections are TCP)**.

Regarding Claim 19, Aronson et al. together with Harris taught the apparatus wherein the commands are Simple Mail Transfer Protocol (SMTP) commands **(Aronson et al. Col. 3, Lines 39-40; SMTP. Harris commands as taught above are in SMTP as well)**.

Conclusion

7. See the enclosed *Notice of References Cited* for a list of prior art that are considered pertinent to the applicant's disclosure but not explicitly relied upon in this action.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher Chan whose telephone number is (571) 270-1927. The examiner can normally be reached on Monday-Friday from 9AM to 5PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeff Pwu, can be reached on 571-272-6798. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Chan

August 28, 2007

JEFFREY PWU
SUPERVISORY PATENT EXAMINER